PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-305662

(43)Date of publication of application : 22.11.1996

(51)Int.Cl. G06F 15/00
G06F 13/00

(21)Application number : 07-108408

(22)Date of filing : 02.05.1995

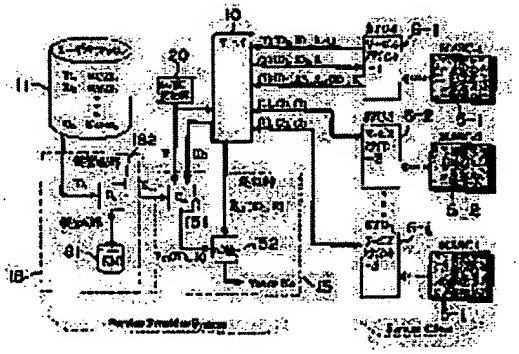
(71)Applicant : FUJITSU LTD

(72)Inventor : AKIYAMA RYOTA
MUNAKATA AKIO
KOGA YUZURU
ISHIZAKI MASAYUKI

(54) METHOD AND SYSTEM FOR CLIENT AUTHENTICATION

(57)Abstract:

PURPOSE: To provide the client authentication system where discrimination information used for authentication between a client and a service presenter cannot be stolen by the third person by dynamically generating this discrimination information in both of the system on the client side and the system on the service prersenter side.



CONSTITUTION: A key management part 18 of a system on the service presenter side generates an individual key K corresponding to a MASC 5 conected to a service client 6, which requests access, and reports this individual key K to an authentication part 15. This individual key K is preliminarily stored in the MASC 5. A random number generator 20 generates random numbers R and not only transmits them to the MASC 5 but also reports them to the authentication part 15. The MASC 5 ciphers these random numbers R by the individual key K and returns them to the system on the service presenter side. Meanwhile, a ciphering part 151 of the authentication part 15 ciphers random numbers R by the individual key K. A comparator 152 of the authentication part 15 compares data ciphered by the ciphering part 151 and ciphered data transmitted from the MASC 5 with each other; and if they are equal

with each other, the access request from the MASC 5 is confirmed.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－305662

(43)公開日　平成８年(1996)11月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０	9364－5L	Ｇ０６Ｆ	15/00	３３０Ｃ
	13/00	３５１	7368－5E		13/00	３５１Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 22 頁）

(21)出願番号　特願平7－108408

(22)出願日　平成７年(1995)５月２日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　宗像　昭夫
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　遠山　勉　（外１名）

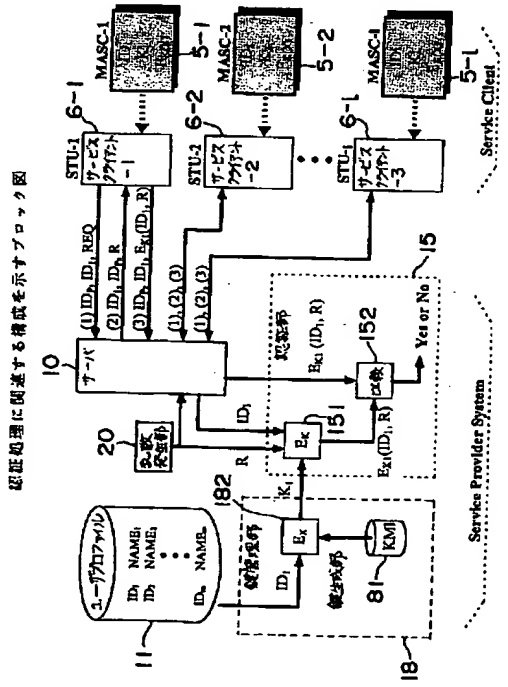
最終頁に続く

(54)【発明の名称】　クライアント認証システムおよび方法

(57)【要約】

【目的】クライアントとサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方おいて動的に作成することにより、これらの第三者による盗用が不可能となるクライアント認証システムを提供する。

【構成】サービス提供者側システム１の鍵管理部１８は、アクセス要求を行ったサービスクライアント６に接続されたＭＡＳＣ５に対応する個別鍵Ｋを生成し、この個別鍵Ｋを認証部１５に通知する。この個別鍵は、予め、ＭＡＳＣ５にも格納されている。乱数発生器２０は、乱数Ｒを生成して、ＭＡＳＣ５に送信するとともに、認証部１５に通知する。ＭＡＳＣ５は、この乱数を個別鍵によって暗号化して、サービス提供者側システム１に戻す。一方、認証部１５の暗号化部１５１は、乱数Ｒを個別鍵Ｋによって暗号化する。そして、認証部１５の比較器１５２は、暗号化部１５１が暗号化したデータとＭＡＳＣから送信されてきた暗号化データを比較して、両者が一致した場合には、このＭＡＳＣ５からのアクセス要求であると確認する。



【特許請求の範囲】
【請求項１】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、
前記データ供給装置は、
前記クライアントに対応する第１の鍵を出力する鍵出力部と、
前記クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段と、
前記鍵出力部において出力されたされた第１の鍵によって前記乱数を暗号化することによって第１の認証子を出力する第１の暗号化手段と、
前記クライアントに前記乱数を送信する第１の送信手段と、
前記クライアントから第２の認証子を受信する第１の受信手段と、
前記第１の認証子と前記第２の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、
前記クライアントは、
前記データ供給装置にアクセス要求を行うアクセス要求手段と、
前記データ供給装置から送信された前記乱数を受信する第２の受信手段と、
前記第１の鍵と同一の第２の鍵を保持する鍵保持手段と、
前記第２の鍵によって前記乱数を暗号化することによって前記第２の認証子を出力する第２の暗号化手段と、
前記データ供給装置に前記第２の認証子を送信する第２の送信手段とを備えることを特徴とするクライアント認証システム。
【請求項２】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、
前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第１の鍵を生成することを特徴とする請求項１記載のクライアント認証システム。
【請求項３】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送することを特徴とする請求項１記載のクライアント認証システム。
【請求項４】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、
前記クライアントは前記暗号化された前記データを複合化する第１の復号化手段を備えることを特徴とする請求項１記載のクライアント認証システム。
【請求項５】前記データ供給装置は前記データを復号化するための第３の鍵を前記第１の鍵によって暗号化する第３の暗号化手段を備えているとともに、
前記クライアントは前記暗号化された前記第３の鍵を前記第２の鍵によって復号化する第２の複合化手段を備え、
前記第１の復号化手段はこの第２の複合化手段によって復号化された前記第３の鍵によって前記暗号化されたデータを復元することを特徴とする請求項４記載のクライアント認証システム。
【請求項６】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとともに、
一方の格納装置に格納されている前記暗号化されたデータを前記第３の鍵を用いて復号化する第３の復号化手段と、
第３の鍵を更新する鍵更新手段と、
第３の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第３の鍵によって暗号化する第３の暗号化手段と、
第３の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えたことを特徴とする請求項５記載のクライアント認証システム。
【請求項７】前記第３の復号化手段，前記鍵更新手段，前記第３の暗号化手段，及び前記書込手段は一定時間毎に起動することを特徴とする請求項６記載のクライアント認証システム。
【請求項８】前記クライアントは、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成されるとともに、
少なくとも前記鍵保持手段及び前記第２の暗号化手段は前記モジュール部に備えられていることを特徴とする請求項１記載のクライアント認証システム。
【請求項９】データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、
前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、
前記データ供給装置は、このアクセス要求に応じて乱数を発生してこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第１の鍵によって前記乱数を暗号化して第１の認証子に変換し、
前記クライアントは前記第１の鍵と同一内容を有するものとして予め保持している第２の鍵によって前記乱数を暗号化して第２の認証子に変換するとともに、この第２の認証子を前記データ供給装置に送出し、
前記データ供給装置は前記第１の認証子と前記第２の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とするクライアント認証方法。
【発明の詳細な説明】
【０００１】

【産業上の利用分野】本発明は、クライアントからの要求に応じて、映像著作物等のソフトウエアを通信手段を介して配送するシステム（デジタル・オーディオ・インタラクティブ・システム）におけるクライアント認証システム及び認証方法に関する。

【０００２】

【従来の技術】近年、ケーブルテレビジョンシステムや通信衛星を用いた通信システムの構築を背景に、デジタル情報化されたソフトウェア（音声データ，映像データ等，以下、「コンテンツ」という）を各家庭等に配送するサービスが提案されている。このサービスシステムは、ビデオ・オン・デマンド方式等と呼ばれるデジタル・オーディオ・インタラクティブ・システムである。このデジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者とユーザとの間で電話線等を介した通信が行われる。そして、サービス提供者は、ユーザから要求された時刻に要求された内容のコンテンツをこのユーザに配送するとともに、このソフトウェアの使用料金をクレジットカード会社等を通じて当該ユーザに課金し、その一部をコンテンツ供給者に還元するのである。

【０００３】このようなデジタル・オーディオ・インタラクティブ・システムが普及してゆく上で重要な事は、インフラストラクチャーとなるサーバ/ ネットワーク/ ターミナルが低コストで構築されることは勿論であるが、これらを媒介としてユーザに提供されるコンテンツが豊富に準備されなければ、成功とはならないということである。即ち、コンテンツとインフラストラクチャは車の両輪であるので、コンテンツ提供者がコンテンツ提供による利益回収を見込めるとともに不測の損害を被る危険がない仕組みをこのインフラストラクチャに組み込むことにより、コンテンツが集まりやすい環境を整備することが不可欠なのである。なお、このような仕組みは、コンテンツ提供者とユーザとを媒介する供給メディアの種類（広帯域ケーブルネットワーク，衛星システム，移動通信，光メディアパッケージ等）に拘わらず、整備されていなければならない。

【０００４】このような環境の整備がなされることにより、コンテンツ供給者は、安心して気軽に、コンテンツを供給することができるようになる。一方、ユーザは、いつでもどこでも、簡単な手続きによって必要なコンテンツを入手できるようになる。このことが、システムをより一層普及させるために重要なポイントとなっているのである。

【０００５】一方、システム構築に当たっては、誰もが参加できるオープン性が重要であり、既存の標準技術を可能な限り活用する方式を取っていくことが必要である。また、技術の進歩や各種サービスの多様化に対応できる拡張性も持ち合わせたものであることを併せて考慮すべきである。

【０００６】

【発明が解決しようとする課題】以上説明したように、デジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者は、コンテンツ配送を要求してきたユーザが誰であるのかを正確に識別して、確実に課金することができなければならない。即ち、課金を行うために必要なデータ（例えば、クレジットカード番号，銀行口座番号，等）を登録していない第三者がこれらデータを登録しているユーザになりすましてコンテンツの配送を受けてしまうことを、防止しなければならない。そのため、登録されているＩＤコードとコンテンツ配送を行ったユーザのＩＤコードとを照合する認証システムが提案されている。

【０００７】しかしながら、このようなＩＤコードによる認証システムでは、ＩＤコードが第三者によって盗まれた場合においてこの第三者による盗用を防止する手だてはない。なお、ＩＤコードにパスワードを付する方式も提案されているが、盗まれた場合に第三者の盗用が可能であることには変わりがない。

【０００８】そこで、本発明の第１の課題は、ユーザ（クライアント）とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方おいて動的に作成することにより、第三者の盗用が不可能となるクライアント認証システムを提供することである。

【０００９】また、単純なＩＤコードによって認証を行うシステムであるならば、ユーザがこのＩＤコードをマニュアルで入力できるので、コンテンツの配送要求を行った個々人毎の認証も可能であるが、複雑な識別情報を扱う場合であると、識別情報の動的な作成は勿論、マニュアルによる識別情報の入力でさえも不可能となってしまう。従って、従来提案されていた認証システムでは、コンテンツの再生を行う再生装置が自動的に認証作業を実行し、この再生装置毎に認証を行うようになっていた。

【００１０】しかしながら、再生装置毎に認証を行うのであると、複数の再生装置を有している場合には、再生装置毎に課金のためのデータを登録しなければならない。また、自己の課金のためのデータがサービス提供者に登録されている場合であっても、例えば他人に借りた再生装置でコンテンツを再生することは一切できなくなってしまう。このように硬直したシステムであると、上述した理由によりシステム普及はおぼつかない。

【００１１】そこで、本発明の第２の課題は、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着できるモジュールに、認証を行うためのデータ及び機能を持たせたクライアント認証システムを提供することである。

【００１２】

【課題を解決するための手段】

（第１の課題を解決するための手段）本発明によるクライアント認証システムの第１の態様は、上記第１の課題を解決するために、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して配送されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証システムにおいて、前記データ供給装置は、前記クライアントに対応する第１の鍵を出力する鍵出力部と、前記クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段と、前記鍵出力部において出力されたされた第１の鍵によって前記乱数を暗号化することによって第１の認証子を出力する第１の暗号化手段と、前記クライアントに前記乱数を送信する第１の送信手段と、前記クライアントから第２の認証子を受信する第１の受信手段と、前記第１の認証子と前記第２の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段とを備え、前記クライアントは、前記データ供給装置にアクセス要求を行うアクセス要求手段と、前記データ供給装置から送信された前記乱数を受信する第２の受信手段と、前記第１の鍵と同一の第２の鍵を保持する鍵保持手段と、前記第２の鍵によって前記乱数を暗号化することによって前記第２の認証子を出力する第２の暗号化手段と、前記データ供給装置に前記第２の認証子を送信する第２の送信手段とを備えることを特徴とする（請求項１に対応）。

【００１３】前記アクセス要求手段は、前記アクセス要求に際してそのクライアントに設定された固有の識別情報を前記データ供給装置に通知するとともに、前記鍵出力部は、各クライアントに固有の前記識別情報を加工することにより前記第１の鍵を生成するようにしても良い（請求項２に対応）。

【００１４】前記データ供給装置は前記比較手段によって前記両認証子が一致すると判断された場合のみ前記データを前記クライアントに配送するようにしても良い（請求項３に対応）。

【００１５】前記データ供給装置は暗号化された前記データを前記クライアントに配送するとともに、前記クライアントは前記暗号化された前記データを複合化する第１の復号化手段を備えるようにしても良い（請求項４に対応）。

【００１６】前記データ供給装置は前記データを復号化するための第３の鍵を前記第１の鍵によって暗号化する第３の暗号化手段を備えているとともに、前記クライアントは前記暗号化された前記第３の鍵を前記第２の鍵によって復号化する第２の複合化手段を備え、前記第１の復号化手段はこの第２の複合化手段によって復号化された前記第３の鍵によって前記暗号化されたデータを復元するようにしても良い（請求項５に対応）。

【００１７】前記データ供給装置は、前記暗号化されたデータを格納するための複数の格納装置を備えるとともに、一方の格納装置に格納されている前記暗号化されたデータを前記第３の鍵を用いて復号化する第３の復号化手段と、第３の鍵を更新する鍵更新手段と、第３の復号化手段によって復号化されたデータを前記鍵更新手段によって更新された前記第３の鍵によって暗号化する第３の暗号化手段と、第３の暗号化手段によって暗号化されたデータを他の前記格納装置に格納する書込手段とを更に備えるように構成しても良い（請求項６に対応）。このように格納装置を二重化する事によりデータのバックアップができるとともに、暗号化した鍵をその都度更新するので、データのセキュリティを向上させることができる。

【００１８】なお、前記第３の復号化手段，前記鍵更新手段，前記第３の暗号化手段，及び前記書込手段を一定時間毎に起動するようにしても良い（請求項７に対応）。本発明によるクライアント認証方法は、上記第１の課題を解決するため、データを保持するデータ供給装置とこのデータ供給装置から通信インタフェースを介して送出されるデータを受信するクライアントからなるデータ配送システムにおけるクライアント認証方法において、前記クライアントは自己を識別する識別情報を付して前記データ供給装置にアクセス要求を行い、前記データ供給装置は、このアクセス要求に応じて乱数を発生してこの乱数を前記クライアントに送出するとともに、前記識別情報に対応する第１の鍵によって前記乱数を暗号化して第１の認証子に変換し、前記クライアントは前記第１の鍵と同一内容を有するものとして予め保持している第２の鍵によって前記乱数を暗号化して第２の認証子に変換するとともに、この第２の認証子を前記データ供給装置に送出し、前記データ供給装置は前記第１の認証子と前記第２の認証子とを比較して両者が一致した場合に前記クライアントからのアクセス要求があったことを認証することを特徴とする（請求項９に対応）。

（第２の課題を解決するための手段）本発明の前記クライアント認証システムの第２の態様は、前記第１の態様におけるクライアントを、前記データを受信する本体部とこの本体部に対して着脱自在に設けられたモジュール部とから構成するとともに、少なくとも前記鍵保持手段及び前記第２の暗号化手段は前記モジュール部に備えるように構成したことを特徴とする（請求項８に対応）。なお、上述の識別情報を使用する場合には、この識別情報はこのモジュール部に格納しておく。また、上述の第１の複合化手段及び第２の複合化手段を設ける場合には、これら複合化手段をこのモジュール部に格納する。

【００１９】

【作用】本発明の第１の態様によると、クライアントのアクセス要求手段がデータ供給装置にアクセス要求を行うと、このアクセス要求に応じて、データ供給装置の乱数発生部が乱数を発生するとともに、鍵出力部がこのクライアントに対応する第１の鍵を出力する。そして、第

１の通信手段は、アクセス要求元のクライアントに乱数を送信する。また、第１の暗号化手段は、鍵出力部において出力された第１の鍵によって乱数を暗号化することにより、第１の認証子を出力する。一方、クライアントの第２の受信手段が乱数を受信すると、第２の暗号化手段は、鍵保持手段が保持している前記第１の鍵と同一の第２の鍵によってこの乱数を暗号化することにより、第２の認証子を出力する。この第２の認証子は、第２の送信手段によってデータ供給装置に送信される。データ供給装置の第１の受信手段がこの第２の認証子を受信すると、比較手段が第１の認証子と第２の認証子とを比較して、両者が一致している場合に当該クライアントからのアクセス要求であると認証する。従って、通信インタフェース上で送信される識別のための情報（認証子）は暗号化されたものであって、その暗号化された結果は乱数に従って変化するので一定にはならない。そのため、第三者による盗用が不可能になる。

【００２０】本発明の第２の態様によると、クライアントを構成する各構成部のうち、認証に必要なデータを保持する構成部（鍵保持手段）や認証に必要な処理を行うための構成部（第２の暗号化手段）のみを、本体部から着脱自在に設けたモジュール部に備えるようにしたので、誰の所有による本体部であっても、ユーザが自分のモジュール部を接続してデータの配送を受けることができる。

【００２１】

【実施例】以下、図面に基づいて、本発明の一実施例の説明を行う。本実施例は、本発明によるクライアント認証システムを、デジタル・オーディオ・インタラクティブ・システムに適用したものである。なお以下の説明においては、コンテンツを再生するためのコンテンツ再生装置のことを、「サービスクライアント」という。

《実施例の構成》

（システムの全体構成）本実施例によるデジタル・オーディオ・インタラクティブ・システムを図１に示す。このシステムは、多数のコンテンツを格納するとともにこのコンテンツを配送するためのサービス提供者側システム１と、コンテンツを再生するための多数の端末とから、構成されている。この端末には、パーソナルコンピュータ２，サービスクライアント６ａ，６ｂ，及びＤＶＤプレーヤ８が含まれている。また、パーソナルコンピュータ２にはリムーバブルディスク装置３が接続されている。また、第１のサービスクライアント６ａには、ＳＣＳＩインタフェースを介して光磁気ディスクドライブ４が接続されている。ＤＶＤプレーヤ８を除く各端末は、上位サービスレイヤインタフェースＳ１，及びアプリケーションサービスレイヤインタフェースＳ２を介して、サービス提供者側システム１に接続されている。

【００２２】これら上位サービスレイヤインタフェースＳ１，及びアプリケーションサービスレイヤインタフェースＳ２は、図２に示すＤＡＶＩＣ 1.0システムリファレンスモデルによって定義されたインタフェースである。この上位サービスレイヤインタフェースＳ１は、コンテンツを配送するためのインタフェースであり、具体的には、ケーブルテレビジョンシステムのケーブル，衛星回線，ＩＳＤＮ等である。また、アプリケーションサービスレイヤインタフェースＳ２は、アクセス制御情報を交換するためのインタフェースであり、ケーブルテレビジョンシステムのケーブル，ＩＳＤＮを上位サービスレイヤインタフェースＳ１と兼用することができる他、アナログ電話網を用いることができる。

【００２３】なお、図１に示した（Ｓ１）は、物理的運搬を意味する。即ち、サービス提供者から購入したコンテンツ入りのフロッピーディスクを運搬して、パーソナルコンピュータ１のリムーバブルディスク装置３にロードしたり、サービス提供者から購入したコンテンツ入りのビデオディスクを運搬して、ＤＶＤプレーヤ８にロードすることを意味する。このような物理的運搬も、Ｓ１のインタフェースに該当する。同様に、制御情報をＦＡＸ，メール等によって送信することも、Ｓ２のインタフェースに該当する。

【００２４】本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供者又はサービス提供者から提供される有料のコンテンツまたは機密情報を第三者から容易に傍受されることを防ぐ目的のために、サービス提供者側システム１とサービスクライアント６との間に、セキュリティ機構を設けた。このセキュリティ機構は、サービス提供者側システム１から供給されるコンテンツが第三者によって悪用されたり転用されることを防止するために、このコンテンツを暗号化してサービスクライアント６に提供する。即ち、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、図２に示したDAVIC 1.0システムリファレンスモデルに基づき、セキュリティ・アンド・アクセス・コントロール機能を、サービス提供者側システム１及びサービスクライアント６に置いたのである。

【００２５】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、サービスクライアント６に復号化機能を持たせるために、模倣や改造が難しいハードウェア機構を一部採用し、認証及び秘匿を実現した。

【００２６】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、ユーザへの利便性を考慮し、復号化機能を実現するアルゴリズム、鍵管理、認証、秘匿、および課金に関する情報などユーザのセキュリティに付随する機能を、利用者が携帯可能なモジュール（以後、「ＭＡＳＣ：Media Access and Security Card」と呼ぶ）５に収め、このＭＡＳＣ５をサービスクライアント６に脱着可能とした。そのた

め、このＭＡＳＣ５を何れかのサービスクライアント６に装着することにより、別個のサービスクライアント６であっても同様のサービスを享受することが可能となる。

【００２７】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、他の標準化作業を尊重するため、サービスクライアント６側の認証方式は、ISO/IEC9798-2 に準拠した。また、鍵管理方式は、B-MACスクランブル放送で採用されている方式に準拠した。また、暗号登録方式は、ISO/IEC 9979に準拠し、鍵サイズおよび入出力データサイズのみ規定するとともに処理アルゴリズムは規定しないものとした。また、ＭＡＳＣ５のサービスクライアント６との物理インタフェースは、DVB 方式案の一部を変更して採用した。

【００２８】また、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいては、コンテンツ提供形態の多様化（ケーブル、衛星システム、パッケージ等）に対応できるように、拡張性の高いデータ構造、処理方式を採用した。

【００２９】＜サービス提供者側システムの構成＞次に、図３を参照して、データ供給装置としてのサービス提供者側システム１の内部構成を説明する。図３に示すように、サービス提供者側システム１は、サーバ１０と、このサーバ１０と各々バス接続されたユーザプロファイル１１，第１データファイル１２，第２データファイル１３，デジタル署名部１４，認証部１５，鍵更新処理部１６，鍵管理部１８，及び乱数発生器２０と、サーバ１０に夫々接続された衛星回線Ｓ，ケーブルテレビジョンシステムのケーブルＣ，及び電話網Ｎと、鍵更新処理部１６に接続された鍵更新タイマ１７と、鍵管理部１８に接続されたサービスプロバイダＩＤ記憶部１９とから、構成されている。

【００３０】第１の送信手段及び第１の受信手段としてのサーバ１０は、サービス提供者側システム１全体の制御を行うとともに、衛星回線Ｓ，ケーブルテレビジョンシステムのケーブルＣ，電話網Ｎを介してサービスクライアント６と通信を行う処理装置である。

【００３１】ユーザプロファイル１１は、各ＭＡＳＣのＩＤが登録されているデータベースである。第１データファイル１２は、暗号化された多数のコンテンツ及びそれらのＩＤ（タイトルＩＤ）を格納するデータベースである。第２データファイル１３は、この第１データファイル１２に格納されていたコンテンツを別の鍵を用いて再暗号化したもの及びそれらタイトルＩＤを格納するデータベースである。即ち、これらのデータファイル１２，１３に格納されるコンテンツは、一定時間毎に再暗号化されて、一方のデータファイルから他方のデータファイルに移されるのである。なお、これらデータファイル１２，１３に格納されるコンテンツには、予めＭＰＥＧ－２規格により圧縮処理がなされている。

【００３２】ディジタル署名部１４は、ユーザに対する課金額に対応した一定範囲のコンテンツ再生を許可するデータを、このデータが正しいことを論理的に証明するデジタル署名情報を付して、サービスクライアント６に送信する部分である。

【００３３】認証部１５は、当該サービス提供者側システム１に対して通信を行ってきたサービスクライアントに装着された個々のＭＡＳＣ５がユーザプロファイル１１にそのＩＤが登録されているどのＭＡＳＣ５であるのかを調べる作業を行う。

【００３４】乱数発生手段としての乱数発生器２０は、この認証部１５の作業において用いられる乱数を発生する。鍵出力部としての鍵管理部１８は、認証部１５におけるＭＡＳＫの識別に用いる鍵（第１の鍵）を、ユーザプロファイル１１に登録されているＭＡＳＣのＩＤから生成するとともに、各データファイル１２，１３に格納されている暗号化されたコンテンツを復元するための鍵（第３の鍵）を、対応するタイトルＩＤに基づいて生成する。

【００３５】サービスプロバイダＩＤ記憶部１９は、この鍵管理部１８における鍵生成に用いられる当該サービス提供者側システムのＩＤ（サービスプロバイダＩＤ：ＩＤＰ）を保持しているメモリである。

【００３６】鍵更新処理部１６は、一方のデータファイル１２，１３に格納されているコンテンツを鍵管理部１８において生成されたタイトルＩＤに基づいて復元するとともに新たな鍵を作成し、復元されたコンテンツをこの新たな鍵によって暗号化して他方のデータファイル１２，１３に格納する。

【００３７】鍵更新タイマ１７は、この鍵更新処理部における処理のタイミングを規定するタイマである。

＜サービスクライアントシステムの構成＞次に、図４を参照して、サービスクライアントシステムの構成を説明する。

【００３８】図４に示すように、サービスクライアントシステムは、衛星回線からの電波を受信するパラボラアンテナ２２と、このパラボラアンテナ２２に接続された衛星デコーダ２３と、ケーブルテレビジョンシステムのケーブルに接続されたＣＡＴＶアダプタ２６と、光磁気ディスクドライブ４と、これら衛星デコーダ２３，ＣＡＴＶアダプタ２６，及び光磁気ディスクドライブ４に接続されたデータセレクタ３８と、このデータセレクタ３８に接続された本体部としてのサービスクライアント６と、このサービスクライアント６に装着されたモジュール部としてのＭＡＳＣ５と、電話網Ｎに接続されたモデム５７とから、構成されている。

【００３９】衛星デコーダ２３は、パラボラアンテナ２２によって受信された信号を復調する復調回路２４と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ２５とから、構成されている。デコーダ

２５の出力端子は、データセレクタ３８の第１コネクタに接続される。

【００４０】ＣＡＴＶアダプタ２３は、ケーブルから受信された信号を復調する復調回路２７と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ２８とから、構成されている。デコーダ２８の出力端子は、データセレクタ３８の第２コネクタに接続される。

【００４１】光磁気ディスクドライブ４は、データセレクタ３８の第４コネクタに接続されたエンコーダ３５と、このエンコーダ３５によってエラー訂正及びビットの並び替えがなされたデータを変調する変調回路３４と、光磁気ディスク３０に対してデータの書込／読み出しを行うピックアップ３１と、ピックアップ３１によって読み出されたデータを復調する復調回路３２と、復調された信号のエラー訂正及びビットの並び替えを実行するデコーダ３３と、光磁気ディスク３０を回転させるとともにピックアップ３１をトラッキングさせるドライブ回路３６とから、構成されている。デコーダ３３の出力端子は、データセレクタ３８の第３コネクタに接続される。

【００４２】データセレクタ３８は、第１乃至第３コネクタから入力したデータを第４コネクタ又は第５コネクタに出力する。そのために、データセレクタ３８は、第１乃至第３の何れかのコネクタに接続線を接続するかを選択するスイッチＳＷ１と、第４又は第５の何れかのコネクタに接続線を接続するかを選択するスイッチＳＷ２とを備えている。

【００４３】サービスクライアント６は、データセレクタの第５コネクタに接続されたＤＬ４０，ホストＣＰＵ４１，及びスイッチ４２と、スイッチ４２に接続されたデマルチプレクサ４３と、このデマルチプレクサ４３に接続された画像用ＭＰＥＧ伸長回路４４と、この画像用ＭＰＥＧ伸長回路４４に接続されたＤ／Ａ変換器４７と、デマルチプレクサ４３に接続された音声用ＭＰＥＧ伸長回路４５と、この音声用ＭＰＥＧ伸長回路４５に接続されたＤ／Ａ変換器４８と、両ＭＰＥＧ伸長回路４４，４５に接続された同期回路４６と、ホストＣＰＵ４１に接続されたセクタペイロード対向テーブル４９と、モデム５７に接続されたインタフェース５０とから、構成されている。

【００４４】ＤＬ４０は、ディレイライン装置であり、トグルバッファ又はＦＩＦＯメモリから構成された帯域変換装置である。スイッチ４２はＣＰＵ４１からの指示に従い、データセレクタ３８からの信号線又はＭＡＳＣ５からの信号線をデマルチプレクサ４３に接続する。また、スイッチ４２は、ＣＰＵ４１からの指示に応じて、回路を開く。

【００４５】ホストＣＰＵ４１は、当該サービスクライアント６全体の制御を行う制御装置である。また、ホストＣＰＵ４１は、データセレクタ３８から受信したコンテンツが予め暗号化されているかどうかを解析する。そして、暗号化がなされていないのであればデータセレクタ３８からの信号線をデマルチプレクサ４３に接続させる指示をスイッチ４２に対して行い、暗号化がなされているのであればＭＡＳＣ５からの信号線をデマルチプレクサ４３に接続させる指示をスイッチ４２に対して行うとともに、ＭＡＳＣ５に対して復号化を指示する。なお、ホストＣＰＵ４１は、ＭＡＳＣ５の制御ＣＰＵ５１からの指示があった場合には、コンテンツが暗号化されている場合であっても、スイッチ４２に対してデータセレクタからの信号線をデマルチプレクサ４３に接続させる指示を行う。また、ホストＳＰＵ４１は、データサレクタ３８からコンテンツを構成する各フレームを受信する毎に、ＭＡＳＣ５に対して通知を行う。

【００４６】デマルチプレクサ４３は、コンテンツ中の音声データフレーム及び画像データフレームを分離する。そして、画像データフレームを画像用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４に出力し、音声データフレームを音声用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４５に出力する。

【００４７】ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４，４５は、ＭＰＥＧ規格で圧縮されたままの状態で送信されて来た画像データフレーム，又は音声データフレームを伸長して、画像又は音声を出力可能なフォーマットに復元する回路である。これらＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４，４５においてデータフレームの伸長をする際には、同期回路４６によって出力の同期がとられる。即ち、同期回路４６から出力される同期信号に同期して、各ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４，４５は、伸長されたデータフレームを出力するのである。

【００４８】画像用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４４からの出力は、Ｄ／Ａ変換器４７によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアント２に接続されている図示せぬＴＶモニタ装置に向けて出力される。また、音声用ＭＰＥＧ伸長回路（ＭＰＥＧ－２）４５らの出力は、Ｄ／Ａ変換器４８によってアナログ信号に変換される。このアナログ信号は、当該サービスクライアントに接続されている図示せぬスピーカに向けて出力される。

【００４９】セクタペイロード対応テーブル４９は、光磁気ディスク３０の各セクタとフレームとの関係を対応させているテーブルである。即ち、光磁気ディスクドライブ４からのコンテンツを読み出している場合において、ホストＣＰＵ４１によって各フレームが読みとられる毎に、このセクタペイロード対応テーブル４９によってセクタとの対応が調べられるのである。そして、現在のセクタから全てのフレームが読み出された時には、セクタコントローラ３７に対して、ピックアップ３１のトラッキングを行うべき旨が指示されるのである。

【００５０】第２の受信手段及び第２の送信手段としてのインタフェース５０は、モデム５７と電話網Ｎ（Ｓ２）を介して、サービス提供者側システム１のサーバ１０と通信を行い、制御情報の送受信を行う。

【００５１】次に、ＤＬ４０，ホストＣＰＵ５１，スイッチ４２，及びインタフェース５６に接続されるＭＡＳＣ５の説明を行う。サービスクライアント６に提供される各種コンテンツは、衛星通信の様に入手が容易な通信媒体を介して配送されることがあるので、その再生に対する課金方法を如何にするかが問題となる。また、このような通信媒体を介して配送されるコンテンツは第三者による盗用を防止するために予め暗号化された状態で流通されるので、これを復号化する必要がある。そのため用いられるのがＭＡＳＣ５である。即ち、ＭＡＳＣ５は、ホストＣＰＵ４１からの指示に応じて、ＤＬ４０を介して受信したコンテンツを復号化してスイッチ４２に送信する。また、ＭＡＳＣ５は、ホストＣＰＵ４１がフレーム４１を受信する毎に行う通知をカウントして、課金カウンタ値Ｘを減算する。この課金カウンタ値Ｘとは、ユーザがサービス提供者側システムのデジタル署名部１４に対して代金支払いを了承することによって当該ＳＤ回路に書き込まれたポイントである。ＭＡＳＣ５は、この課金カウンタ値Ｘが０になった時に、ホストＣＰＵ４１に対して、スイッチ４２を開かせるのである。

【００５２】なお、このＭＡＳＣ５は、サービスクライアント６のカードスロット（たとえばＰＣＭＣＩＡ準拠のカードスロット）内に着脱自在に装着されたＩＣカードの形態で実現される。このようなＩＣカードの形態にしておけば、ＳＤ回路の運搬が容易となる。

【００５３】このＭＡＳＣ５は、相互にバス接続された制御ＣＰＵ５１，ＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）５３，課金情報記憶部５５，ＲＯＭ５７，並びにＩ／Ｏ装置５２，５４，及び５６から構成されている。

【００５４】制御ＣＰＵ５１は、サービスクライアント６内のホスト制御ＣＰＵ１４に接続されており、ホストＣＰＵ４１からの指示に応じてＤＥＳ５３に対して復号化処理を実行させる。また、制御ＣＰＵ５１は、ホストＣＰＵ４１からのフレーム受信通知に応じて課金部５５内に格納されている課金カウンタ値Ｘを減算するとともに、この課金カウンタ値Ｘが０になったときは、ＣＰＵ４１に対して、スイッチ４２を開かせる。また、制御ＣＰＵ５１は、Ｉ／Ｏ装置５６，インタフェース５０及びモデム５７を介してサービス提供者側システム１との間で通信を行って、アクセス要求，ディジタル署名，及びユーザ認証のために必要な処理を行う（アクセス要求手段に対応）。

【００５５】鍵保持手段としてのＲＯＭ５６は、この制御ＣＰＵ５１における処理に必要な諸データ（例えば、当該ＭＡＳＣ５を識別するための識別ＩＤ$_i$［固有の識別情報］，当該ＭＡＳＣ５に固有のものとして備えられた個別鍵Ｋ$_i$［第２の鍵］）を記憶しているメモリである。

【００５６】課金情報記憶部５５は、上述した課金カウンタ値Ｘを格納しているメモリである。なお、課金情報記憶部５５内において、課金カウンタ値Ｘは暗号化されている。従って、ユーザがこの課金情報記憶部５５を解析して課金カウンタ値Ｘを書き換えることは、不可能である。

【００５７】第２の暗号化手段，並びに第１及び第２の複合化手段としてのＤＥＳ７は、Ｉ／Ｏ装置５２を介してＤＬ４０から受け取ったコンテンツを復号化する機能，及び制御ＣＰＵ５１が行うディジタル署名及びユーザ認証に際して必要な暗号化及び復号化を行う機能を有する。ＤＥＳ７により復号化されたコンテンツ（画像フレーム，音声フレーム）は、Ｉ／Ｏ装置５４を通じて、スイッチ４２に送出される。

《実施例における処理内容》次に、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいて、サービス提供者側システム１とサービスクライアント６との間で実行される制御処理を、フローチャート及びこのフローチャートの各ステップにおいて実現される機能を示すための機能ブロック図を参照して、説明する。

【００５８】サービスクライアント６がサービス提供者側システム１管理の情報にアクセスする場合，安全な通信制御手段が必要となる．これはサービスクライアント６とサービス提供者側システムとの間を結ぶＳ１とＳ２の形態により異なる。

【００５９】（コンテンツ情報送信制御処理）先ず最初に、サービスクライアント６側からサービス提供側システム１に対して何れかのコンテンツの配送を要求する際の制御処理について説明する。この場合、Ｓ１，Ｓ２のインタフェースが秘密保持性が高い通信媒体であるか否かによって、制御を異にする。なぜならば、秘密保持性が低い通信媒体によってコンテンツを配送する場合には、第三者による盗用やデータ改ざんを防ぐために暗号化する処理が不可欠だからである。

【００６０】＜秘密保持性が高い通信媒体によるコンテンツ情報供給制御＞図５は、Ｓ１，Ｓ２の形態を、例えば光ファイバケーブル（ケーブルテレビジョンシステムのケーブル，等）のように、データ盗聴やデータ改ざんが比較的困難な信頼できるネットワークとした場合における制御内容を示す．この場合、サービスクライアント６側の不正アクセスのみが問題となる。従って、アクセス権確立のための認証が重要となる．

【００６１】この場合の運用手順の概略を説明すると、最初にユーザは、サービスクライアント６にＭＡＳＣ５を挿入する。すると、サービスクライアント６は、ＭＡＳＣ５の識別ＩＤ（ＩＤ$_i$）を読み取り、その識別ＩＤ

（ＩＤi）をサービス提供者側システムへ通知する。すると、サービス提供者側システム１は、何れのＭＡＳＣ５であるかを認証する。次に、サービス提供者側システム１は、要求されたコンテンツをサービスクライアント６に向けて配送し、課金システムを動作させる。その結果、サービスクライアント６は、コンテンツを入手する。

【００６２】［アクセス要求］図５における最初のステップ０１では、サービスクライアント６は、サービス提供者側システム１に対してアクセス要求を行う。この前提として、サービスクライアント６が所有するＭＡＳＣ５には、モジュール固有の識別ＩＤ（ＩＤi），個別鍵Ｋi，及び認証アルゴリズムＥＫ(X)が安全に格納されている。

【００６３】ユーザは、このＭＡＳＣ５を任意のサービスクライアント６へ接続し、図示せぬ操作キーを介してサービス提供者側システムの識別ＩＤ（サービスプロバイダＩＤ：ＩＤp）を入力する。すると、図６（１）に示すように、サービスクライアント６は、サービス提供者側システムへのデータファイルアクセス要求コマンド，及びモジュール固有の識別ＩＤに、サービス提供者側システムのデスティネーション〔サービス提供者側システムの識別ＩＤ（ＩＤp）とサービスクライアント６の識別ＩＤ（アドレス）とを結合したもの〕を付して、Ｓ２インタフェースを介してサービス提供者側システム１に送信する。なお、この時、サービスクライアント５は、配送を求めるコンテンツのタイトルＩＤ（ＩＤＴ）を、サービス提供者側システム１に送信する。

【００６４】［認証処理］図５における次のステップ０２では、サービス提供者側システム１によるサービスクライアントの認証処理を行う。このサービスクライアント認証は、当事者以外の第三者によるサービス提供者側システム１のデータファイルへの不正アクセス阻止を目的に実行される。ここでは、ISO/IEC 9798-2を利用し、当事者間で互いに共有する秘密の鍵データが同一であることにより認証を行う。

【００６５】サービス提供者側システム１がアクセス要求をしたサービスクライアント６の正当性を認証する場合には、図６に示すような手順で認証処理を行う。尚、この認証のための通信は、Ｓ２インタフェースを介して行われる。

【００６６】サービス提供者側システム１のサーバ１０がサービスクライアント６からのアクセス要求を受信すると（１）、鍵管理部１８内の第１鍵生成部（鍵出力部）１８２は、受信したＭＡＳＣ識別ＩＤ（ＩＤi）がユーザプロファイル１１に登録されていることを確認し、ユーザプロファイル１１内の当該識別ＩＤ（ＩＤi）を基に、プロバイダ管理の第１マスタ鍵８１を使ってクライアント個別鍵（第１の鍵）Ｋiを生成する。この第１マスタ鍵８１は、ＭＡＳＣ５内に格納されている個別鍵（第２の鍵）Ｋiが生成された際に用いられたマスタ鍵と同一である。従って、受信したＭＡＳＣ識別ＩＤ（ＩＤi）とユーザプロファイル１１内に登録されている識別ＩＤ（ＩＤi）とが同一である限り、ＭＡＳＣ５内の個別鍵Ｋiと全く同じクライアント個別鍵Ｋiが生成されることになる。

【００６７】これと同時に、サービス提供者側システム１内の乱数発生部２０は、乱数Ｒを発生する。この乱数Ｒは、認証部１５に入力されるとともに、サーバ１０にも入力される。サーバ１０は、この乱数Ｒにサービスクライアント向けデスティネーション〔サービスクライアント６の識別ＩＤ（アドレス）とサービス提供者側システムの識別ＩＤ（ＩＤP）とを結合したもの〕を付けて、サービスクライアント６へ送信する（２）。

【００６８】サービス提供者側システム１からの情報を受信したサービスクライアント６は、情報に含まれる乱数ＲをＭＡＳＣ５に与える。すると、ＭＡＳＣ５は、ＭＡＳＣ識別ＩＤ（ＩＤi）に乱数Ｒを結合して、これを個別鍵Ｋiによって暗号化することにより、第２の認証子を生成する。サービスクライアント６は、この第２の認証子にサービス提供者側システムのデスティネーションを付して 再びサービス提供者側システム１へ送り返す（３）。

【００６９】このクライアント情報を受信したサービス提供者側システム１は、この情報に含まれる第２の認証子を、認証部１５内の比較器（比較手段）１５２へ設定する。更に、認証部１５内の第１暗号化部（第１の暗号化手段）１５１は、サービスクライアント５から受信したＭＡＳＣ識別ＩＤと乱数発生部２０から受信した乱数Ｒとを結合して、これを鍵生成部１８２にて生成されたクライアント個別鍵Ｋiによって暗号化することにより、第１の認証子を生成する。第１暗号化部１５１は、この第１の認証子を比較器１５２へ設定して、先に設定した第２の認証子と比較させる。比較器１５２において両認証子が一致すれば、サービスクライアント５及びサービス提供者側システム１間に同一の個別鍵Ｋiが保有されていることになるので、認証部１５は、当該サービスクライアントを通信当事者として認証し、後の処理を可能とする。これに対して、両認証子が相違している場合には、そのＭＡＳＣ５に対応する課金用データが登録されていないサービスクライアントであると判断して、後の処理を禁止する。　このように、本実施例による認証方式によると、認証の対象となる個別鍵Ｋi自体がインタフェース上を送信されるのではなく、アクセス要求の都度生成される乱数をこの個別鍵Ｋiで暗号化した認証子が送信されるだけである。従って、第三者が乱数Ｒを盗んだとしても、個別鍵Ｋiの内容を知らない限り、認証子を生成することは不可能である。また、認証子自体を盗んだとしても、既に正規のユーザに対する認証が済んでいる場合には、この認証子に対する乱数Ｒは認証

部１５にセットされていないので、当該認証子は既に無効となっている。このように何れにしても第三者の不正なアクセスは、阻止されるのである。

【００７０】なお、サービスクライアント６がサービス提供者側システム１を認証するときには、上記のサービスクライアント６及びサービス提供者側システム１の立場を入れ換えて同様な手順を実行することにより、サービスクライアント６がサービス提供者側システム１を認証することが可能となる。

【００７１】また、認証プロセスで用いるパラメータは、認証子の生成アルゴリズムにより異なる。例えば生成アルゴリズムにＤＥＳ(DATA ENCRYPTION STANDARD)を採用した場合，以下の通りである。

【００７２】

乱数Ｒ　　：32 ビット

ＭＡＳＣ識別ＩＤ：32 ビット(ＥＣＢ入力時には残り32ビットはパディングする)

個別鍵K_i　　：56 ビット

マスタ鍵ＫＭ　　：168ビット(56 ビット×3)

サービス提供者側システム１の利用モード：TRIPPLE ECB(ELECTRONIC CODE BOOK)(個別鍵生成，乱数生成)

サービスクライアントの利用モード：ECB(認証処理)

［コンテンツ情報配送処理］図５における次のステップ０３では、サービスクライアント６からのコンテンツ情報配送処理を行う。即ち、サービス提供者側システム１は、サービスクライアント５から要求されたタイトルＩＤ（ＩＤＴ）に対応するコンテンツ（暗号化コンテンツ）を、何れかのデータファイル１２，１３から読み出して復号化する。そして、Ｓ１インタフェースを介して、復号化されたコンテンツをサービスクライアント６に送信するのである。

【００７３】コンテンツを受け取ったサービスクライアント６は、これを一旦光ディスクドライブ４に送信して光ディスク３０に書き込むか、そのままＣＰＵ４２に流す。ホストＣＰＵ４２はこのコンテンツが暗号化されていないものであると解析して、スイッチ４３をデータセレクタ側に切り換える。従って、コンテンツはそのままデマルチプレクサ４３にて画像フレームと音声フレームに分離されて、夫々ＭＰＥＧ伸長回路４４，４５にて伸長され、ＤＡ変換器４７，４８にてアナログ信号に変換される。そして、画像信号は図示せぬＴＶモニタへ送信され、音声信号は図示せぬスピーカへ送信される。

【００７４】また、ホストＣＰＵ４１は、コンテンツを構成する各フレームを読み込む毎に、ＭＡＳＣ５内の制御ＣＰＵ５１に通知を行う。この制御ＣＰＵ５１は、通知の数をカウントして、課金情報記憶部５５内の課金カウント値Ｘを減算する。そして、この課金カウント値Ｘが０になると、制御ＣＰＵ５１は、ホストＣＰＵ４１に対して、スイッチを４２を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止されるのである。

【００７５】＜一般のネットワークによるコンテンツ情報供給制御＞図７は、Ｓ１，Ｓ２の形態を、無線路や様々な迂回路を経由する一般のネットワーク形態とした場合における制御内容を示す。この形態では、データ盗聴やデータ改ざん行為が十分起こり得るので、上述のサービスクライアント認証処理の他、データ暗号化を如何に行うかが重要である.

【００７６】この場合の運用手順の概略を説明すると、最初に利用者は、サービスクライアント６にＭＡＳＣ５を挿入する。すると、サービスクライアント６は、ＭＡＳＣ５の識別ＩＤ（ID_i）を読み取り、その識別ＩＤ（ID_i）をサービス提供者側システムへ通知する。すると、サービス提供者側システム１は、何れのＭＡＳＣ５であるかを認証する。次に、サービス提供者側システム１は、サービスに必要な鍵（KG_j）をサービスクライアント６に配送する。このようにして、サービスクライアント６は、必要な鍵（KG_j）を入手する。その後、サービス提供者側システム１は、要求されたコンテンツをサービスクライアント６に向けて配送し、課金システムを動作させる。その結果、サービスクライアント６は、この鍵（KG_j）を利用してコンテンツを入手する。

【００７７】［アクセス要求］図７における最初のステップ１１では、サービスクライアント６は、図８に示すように、サービス提供者側システム１に対してアクセス要求を行う。このアクセス要求の内容は、図５におけるステップ０１と同じなので、その説明を省略する。

【００７８】［認証処理］図７における次のステップ１２では、サービス提供者側システム１は、図８に示すように、サービスクライアント６の認証を行う。この認証処理は、図５におけるステップ１２と同じなので、その説明を省略する。

【００７９】［鍵配送処理］図７における次のステップ１３では、サービス提供者側システム１は、図８に示すように、暗号化コンテンツの復元用の鍵（KG_j）の配送を行う。この鍵配送は、暗号化されている各種コンテンツの情報をサービスクライアント６側で円滑に復号させる為に、Ｓ２インタフェースを使って行われる。

【００８０】即ち、サービス提供者側システム１は、サービスクライアント６に装着されたＭＡＳＣ５が発信してきたＭＡＳＣ識別ＩＤ（ID_i）から、クライアント個別鍵K_iを生成しする（このクライアント個別鍵K_iとしてクライアント認証において用いたものを流用しても良い。）。サービス提供者側システム１は、クライアント個別鍵K_i鍵によってサービスプロバイダＩＤ（ＩＤＰ）及びタイトル鍵KG_{1j}を暗号化し、サービスクライアント向けデスティネーション〔サービスクライアント６の識別ＩＤ（アドレス）とサービス提供者側システムの識別ＩＤ（アドレス）とを結合したもの〕を付して、

ＭＡＳＣ５に送信する。サービス提供者側システム１からの暗号化鍵情報は、ＭＡＳＣ５において復号化され、タイトル鍵KG_{1j}が得られる。以後、Ｓ１インタフェースで送られてくる暗号化コンテンツが、このタイトル鍵KG_jによって復号化される。

【００８１】この鍵配送処理の内容を、図９の機能ブロック及び図１０のサブルーチンフローチャートに基づいて説明する。なお、説明の都合上、現時点において第１データファイル１２に暗号化コンテンツが格納されているとし、これを「旧データファイル」と称するものとする。

【００８２】図１０において、最初のステップ２１では、サービス提供者側システム１の鍵管理部１８内に備えられたスイッチＳＷ４を、旧データファイル１２側に切り換える。そして、サービスクライアント５から要求されているタイトルに対応するタイトルＩＤ（ＩＤＴ）を、スイッチＳＷ４を介して旧データファイル１２から読み出す。第２鍵生成部１８４は、読み出したタイトルＩＤ（IDT_j）を第２マスタ鍵１８５に基づいて暗号化し、タイトル鍵（第３の鍵）KG_{1j}を生成する。

【００８３】次のステップ２２では、鍵管理部１８内の第２暗号化部（第３の暗号化手段）１８３は、サービスプロバイダＩＤ記憶部１９から受信したサービスプロバイダＩＤ（ＩＤＰ）と、第２鍵生成部１８４から受信したタイトル鍵KG_jとを、結合する。そして、第２暗号化部１８３は、認証処理時において第１鍵生成部１８２が生成したクライアント個別鍵K_iに基づいて、これらサービスプロバイダＩＤ（ＩＤＰ）及びタイトル鍵KG_{1j}を暗号化し、サーバ１０に転送する。サーバ１０は、受け取ったサービスプロバイダＩＤ及びタイトル鍵KG_{1j}の暗号化情報を、Ｓ２インタフェースを介してサービスクライアント６に配送する。

【００８４】次のステップ２３では、サービスクライアント６は、サービスプロバイダＩＤ及びタイトル鍵KG_{1j}の暗号化情報をＭＡＳＣ５に配送する。ＭＡＳＣ５内の第１復号化部（第２の複合化部）１０１（ＤＥＳ５３）は、ＭＡＳＣ６のＲＯＭ５７に内蔵されている個別鍵K_iを用いてこの暗号化情報を復号化し、サービスプロバイダＩＤ及びタイトル鍵KG_{1j}を獲得する。そして、このサービスプロバイダＩＤ（ＩＤＰ）を比較器１０２にセットする。

【００８５】次のステップ２４では、ＭＡＳＣ６内の比較器１０２は、第１復号化部１０１によってセットされたサービスプロバイダＩＤ（ＩＤＰ）とアクセス要求時に図示せぬ操作キーを介して入力されたサービスプロバイダＩＤ（ＩＤＰ）１０３とを、比較する。そして、両者が一致している場合には、処理をステップ２５に進め、不一致の場合には、処理をステップ２７に進める。

【００８６】ステップＳ２７において、受信不可能である旨がサービスクライアント５側に通知され、Ｓ２インタフェースを介してサービス提供者側システム１のサーバ１０に転送される。

【００８７】次のステップ２８では、サービス提供者側システム１のサーバ１０は、第２暗号化部１８３から受け取ったサービスプロバイダＩＤ（ＩＤＰ）及びタイトル鍵KG_{1j}の暗号化情報を、Ｓ２インタフェースを介して再度ＭＡＳＣ５側へ配送する。その後、処理はステップＳ２３に戻される。

【００８８】これに対して、ステップ２５では、ＭＡＳＣ６内のスイッチＳＷ３が閉じられ、第１復号化部１０１において復元されたタイトル鍵KG_{1j}が第２復号化部（第１の復号化手段）１０４（ＤＥＳ５３）にセットされる。それとともに、受信可能である旨がサービスクライアント５側に通知され、Ｓ２インタフェースを介してサービス提供者側システム１のサーバ１０に転送される。

【００８９】ステップ２６において、サービス提供者側システム１のサーバ１０は、スイッチＳＷ１を閉じて、データファイル１２からタイトル鍵KG_{1j}に対応するタイトルの暗号化コンテンツを読み出す。

【００９０】［コンテンツ情報配送処理］図７のステップ１４において実行されるコンテンツ情報配送処理は、図１０のステップ２６の直後に実行される。

【００９１】即ち、図１１に示すように、サーバ１０は、データファイル１２から読み出した暗号化コンテンツを、Ｓ１インタフェースを介してサービスクライアント６に配送する。サービスクライアント６は、この暗号化コンテンツをＭＡＳＣ５に転送する。ＭＡＳＣ５の第２復号化部１０４（ＤＥＳ５３）は、セットされたタイトル鍵KG_{1j}を用いてこの暗号化コンテンツを復号化する。

【００９２】図４を用いてこの復号化を具体的に説明する。コンテンツを受け取ったサービスクライアント６は、これを一旦光ディスクドライブ４に送信して光ディスク３０に書き込むか、そのままＣＰＵ４２に流す。ホストＣＰＵ４２はこのコンテンツが暗号化されているものであると解析して、スイッチ４３をＭＡＳＣ側に切り換えるとともに、ＭＡＳＣ５の制御ＣＰＵ５１に対して、復号化処理を指示する。この指示に応じて、制御ＣＰＵ５１は、暗号化コンテンツをＤＬ４０及びＩ／Ｏ装置５２を介して読み込み、ＤＥＳ５３（第１復号化部１０１，第２復号化部１０４）によって復号化を行う。このＤＥＳ５３には、インタフェース５０及びＩ／Ｏ装置５６を介して受信したタイトル鍵KG_{1j}がセットされているので、このタイトル鍵KG_{1j}を用いて複合化する。複合化されたコンテンツは、Ｉ／Ｏ装置５４を介してスイッチ４２に送信される。

【００９３】コンテンツは、スイッチ４２からデマルチプレクサ４３に転送され、このデマルチプレクサ４３にて画像フレームと音声フレームに分離されて、夫々ＭＰ

ＥＧ伸長回路４４，４５にて伸長され、ＤＡ変換器４７，４８にてアナログ信号に変換される。そして、画像信号は図示せぬＴＶモニタへ送信され、音声信号は図示せぬスピーカへ送信される。

【００９４】また、ホストＣＰＵ４１は、コンテンツを構成する各フレームを読み込む毎に、ＭＡＳＣ５内の制御ＣＰＵ５１に通知を行う。この制御ＣＰＵ５１は、通知の数をカウントして、課金情報記憶部５５内の課金カウント値Ｘを減算する。そして、この課金カウント値Ｘが０になると、制御ＣＰＵ５１は、ＤＥＳ５３による復号化を中止するとともに、ホストＣＰＵ４１に対してスイッチを４２を開かせる。従って、課金額に対応する使用許可量を越えたコンテンツの使用が阻止されるのである。

【００９５】このように、本実施例のキー配送処理によれば、データファイル１２に格納されている各コンテンツ毎に、別個の復元用鍵（タイトル鍵KG_{1j}）を生成した。従って、同一のユーザが同じキーを用いて他のタイトルのコンテンツを再生することが防止できる。また、このタイトル鍵KG_{1j}は、ＭＡＳＣ５毎に用意された鍵（個別鍵K_i）によって暗号化されるので、第三者が暗号化された鍵を傍受したとしても、タイトル鍵KG_{1j}を復元することは不可能である。従って、第３者の盗用が阻止できる。

【００９６】（ローカル課金処理）次に、コンテンツ情報を再生するために必要な課金カウント値Ｘの加算を申込むためのローカル課金処理を、図１２に基づいて説明する。この課金カウント値Ｘの加算値は、サービスクライアント６からサービス提供者側システム１に対して、代金の銀行口座からの引き落としを条件に申し込まれ、サービス提供者側システム１によってＭＡＳＣ５に書き込まれる。このように、本実施例では、課金カウント値Ｘの管理をＭＡＳＣ５において行っているので、特にデータ改ざん防止に重点が置かれる。よって、サービス供給者側システム１がこの加算値の正当性を証明するために加算値情報に付すデジタル署名が重要となる。従って、サービス提供者側システム１には、予め、ＭＡＳＣ５毎に、暗証番号が登録されているものとする。

【００９７】［アクセス要求］図１２における最初のステップ３１では、サービスクライアント６は、図１３に示すように、サービス提供者側システム１に対してアクセス要求を行う。このとき、サービスクライアント６は、サービス提供者側システム１への課金カウント値増加要求コマンド，及びＭＡＳＣ固有の識別ＩＤに、サービス提供者側システムのデスティネーション〔サービス提供者側システムの識別ＩＤ（サービスプロバイダＩＤ：ＩＤＰ）とサービスクライアント６の識別ＩＤ（アドレス）とを結合したもの〕を付して、Ｓ２インタフェースを介してサービス提供者側システム１に送信する。

【００９８】［認証処理］図１２における次のステップ３２では、サービス提供者側システム１は、図１３に示すように、サービスクライアント６の認証を行う。この認証処理は、図５におけるステップ０２と同じなので、その説明を省略する。

【００９９】［デジタル署名処理及び課金カウント値の書込処理］図１２における次のステップ３３では、サービスクライアント６においてデジタル署名が行われ、次のステップＳ３４では、サービス提供者側システム１による課金カウント値Ｘの補充処理が行われる（図１３参照）。

【０１００】即ち、ユーザによるメッセージの認証は、サービス提供者側システム１とサービスクライアント５との間で、課金に関わるセンシティーブデータをやりとりするときに、通信路上での第三者によるデータの改竄行為やサービスクライアント６でのユーザによるデータ改竄行為を阻止し、当事者間で円滑なトランザクション行為を達成するために、用いられる。ここでは、ISO 8731-1に基づくＭＡＣ(MESSAGE AUTHENTICATION CODE)方式を利用する。

【０１０１】サービス提供者側システム１のデジタル署名部１４は、ユーザの銀行口座から引き落とす金額に対応する補充カウンタ値のデータブロック（DATA OF MENEY）１４０を、送信用フレームＦに格納する。補充カウンタ値のデータブロック（DATA OF MENEY）１４０は、また、当該ＭＡＳＣ５についての加算履歴回数に応じてインクリメントされる通番（ＩＶ）によって署名処理される（ステップ３３）。即ち、排他ＯＲ回路１４２及び第３暗号化部１４３において、暗証番号（ＩＶ）を用いて、補充カウンタ値のデータブロック（DATA OF MENEY）１４０が暗号化されるのである。このような署名処理の最終処理結果（ＭＡＣ）は、サービス提供者側システム１が補充カウンタ値の正当性を証明するためのデータとして、送信用フレームＦに格納される。この送信用フレームＦは、Ｓ２インタフェースを介して、サービスクライアント６に装着されたＭＡＳＣ５に送信される（ステップ３４）。

【０１０２】ＭＡＳＣ５は、受信した送信用フレームＦに対して、サービス提供者側システム１側と同一処理を行う。即ち、送信用フレームＦから補充カウンタ値のデータブロック（DATA OF MENEY）１４０を読み出す。そして、排他ＯＲ回路１０６及び暗号化回路１０６（ＤＥＳ５３）において、補充履歴回数に応じてインクリメントされる通番（ＩＶ）を用いて、補充カウンタ値データブロックの全てに対して署名処理を行う。なお、この通番（ＩＶ）は、通常であれば、サービス提供者側システム１のディジタル署名部１４に格納されている通番（ＩＶ）に同期している。次に、比較器１０７において、署名処理の結果生成されたＭＡＣの値（ＭＡＣ’）と送信用フレームＦに格納されたＭＡＣ１４１の値とを比較する。比較の結果、両値が一致した時には、送信用フレー

ムFに格納された補充カウンタ値のデータブロック（DATA OF MENEY）１４０が正しい金額データであると判断し、スイッチＳＷ６を閉じる。すると、この補充カウンタ値が、課金情報記憶部５５に格納されている課金カウンタ値Ｘに加算される。

【０１０３】以上の結果、ユーザが送信用フレームＦから補充カウンタ値を読み出してこれを書き換えた場合には、この書き換えた補充カウント値が課金カウント値Ｘに加算できなくなってしまうので、不正が防止できる。

【０１０４】このデジタル署名処理に用いられるパラメータは以下の通りである。

暗号化処理　　：DES
署名鍵　　：56ビット
ＭＡＣ　　：32ビット(64 ビット出力の左32ビットを抽出)
金額データ　　：64ビットブロック単位(不足分の32ビットはパディングビットを挿入)

（鍵の更新処理）次に、一定時間毎に、旧データファイル１２に格納されたコンテンツを新規なタイトル鍵KG_{2j}によって暗号化し直して新データファイル１３に格納するための処理を図９のブロック図及び図１４のフローチャートを参照して説明する。

【０１０５】即ち、サービス提供者側システム１で管理する各種タイトルのコンテンツは、それぞれのタイトル鍵KG_{1j}で予め暗号化されているが、同一の鍵で恒久的に暗号化した場合、解読の危険性が高まる。この為、タイトル鍵KG_1の定期的更新を行って、暗号化をし直す必要があるのである。また、新たに追加されたタイトルのコンテンツに対しても、その都度タイトルに応じたタイトル鍵KG_{2j}で暗号化する必要がある。そのため、本実施例では、データファイルを第１のデータファイル１２及び第２のデータファイル１３に分け、一方のデータファイルに現在稼働中の暗号化情報を格納するとともに（旧データファイル）、他方のデータファイルには図１４の鍵の更新処理を実行することにより新たな暗号化コンテンツを格納するのである（新データファイル）。この図１４の処理の前提として、鍵管理部１８の第２マスタキー１８５と鍵更新処理部１６の第２マスタ鍵１６３とは全く同じものであるとする。また、一度使用したタイトル鍵KG_{1j}は再使用を行うことなく使い捨てられるので、タイトル鍵KG_{1j}の生成に用いられる第２マスタ鍵１６３，１８５は、鍵更新の都度変更される。

【０１０６】図１４の処理は鍵更新タイマ１７に設定された周期毎にスタートする。即ち、本実施例では、タイトル鍵KG_{1j}の更新を、プログラムのサイクル及び安全係数を考慮に入れ、例えば一週間毎に行うようにしている。なお、図１４の処理のスタートタイミング，即ち、新タイトル鍵KG_{2j}によって暗号化され直した新コンテンツの新データファイルへ格納するタイミングは、旧データファイル稼働中であることは、言うまでもない。また、第１データファイル１２を旧データファイルとする場合には、スイッチＳＷ１を閉じ、スイッチＳＷ２を開き、スイッチＳＷ４を第１データファイル１２側とし、スイッチＳＷ５を第２データファイル側１３とする。これに対して、第２データファイル１３を旧データファイルとする場合には、これらと全く逆にする。

【０１０７】図１４の処理において最初のステップ４１では、鍵更新処理部１６の復号処理部（第３の復号化手段）１６１に、第２鍵生成部１８４において現在のタイトルＩＤ（IDT_{1j}）に基づいて生成されたタイトル鍵KG_1をセットする。

【０１０８】次のステップ４２では、旧データファイル１２に格納されている当該タイトル鍵KG_1に対応する暗号化コンテンツを鍵更新処理部１６の復号装置１６１にセットして、タイトル鍵KG_1に基づいて復号を行う。

【０１０９】次のステップ４３では、鍵更新処理部１６の第３鍵生成部（鍵更新手段）１６４は、新データファイルに予め格納されている何れかのタイトルＩＤ（IDT_{2j}）を第２マスタ鍵１６３により暗号化して、新タイトル鍵KG_{2j}を生成する。第４暗号化部（第３の暗号化手段）１６２は、復号されたコンテンツを新タイトル鍵KG_{2j}に基づいて暗号化し直す。

【０１１０】次のステップ４４では、第４暗号化部１６２が暗号化し直した暗号化コンテンツを、新データファイル１３に書き込む（書込手段に対応）。次のステップ４５では、鍵更新タイマー１７によってある期限（例えば毎日曜日の深夜以降）まで待ち、各スイッチＳＷ１，２，４，５を切り換える。例えば、第１データファイルを旧ファイルとしていた場合においては、スイッチＳＷ２を閉じ、スイッチＳＷ１を開き、スイッチＳＷ４を更新側に切り換え、スイッチＳＷ５を旧データファイル１２側に切り換える。これより、新データファイル１３に格納されているタイトルＩＤ（IDT_{2J}）を鍵管理部１８に送信可能となり、新データファイル１３に格納されている暗号化コンテンツをサーバ１０に送信可能となるとともに、この新データファイルを旧データファイルとして扱う次回の更新処理が可能となる。このステップ４４の処理が完了すると、処理が図１０のステップ２１に渡される。

【０１１１】（MASC の緊急対策）ユーザ側で万一ＭＡＳＣ５の紛失又は盗難に遭遇した場合、サービス提供者は、緊急に鍵の破壊及びＭＡＳＫ５の再発行を行う。即ち、ユーザは、ＭＡＳＣ５の紛失又は盗難の事実が確認されたなら、電話等の通信手段を使って直ちにサービス提供者にそのむね連絡する。このときユーザは、自身の名前，住所，連絡先をサービス提供者に通知する。次に、サービス提供者は、サービス提供者側システム１のプロファイルデータでユーザを確認後、ユーザに対して電話によるコールバックを行う。そして、サービス提供

者及びユーザ間で確認及び合意がとれれば、サービス提供者は、プロファイルから該当ユーザデータ全てを抹消し、対応するＭＡＳＣ５のＩＤ（ID_i）を永久欠番とする。その後、ユーザは、サービス提供者又は近くの特約店或いは代理店へ行き、再登録の申請を行い、新しいＩＤ（ID_i）付ＭＡＳＣ５を発行してもらう。

【０１１２】

【発明の効果】以上のように構成された本発明のクライアント認証システムの第１の態様によると、ユーザ（クライアント）とサービス提供者との間で認証に用いる識別情報をクライアント側システムとサービス提供者側システムとの双方おいて動的に作成するので、第三者の盗用が不可能となる。

【０１１３】また、本発明のクライアント認証システムの第１の態様によると、ユーザが容易に携帯できるとともに複数の再生装置に対して共通に装着されるモジュールに、認証を行うためのデータ及び機能を持たることができるので、再生装置が自己のものか否かに拘わらずコンテンツを再生できるとともに、サービス提供者は確実にコンテンツ再生代金を徴収することができる。

【図面の簡単な説明】

【図１】　本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図

【図２】　図１のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図

【図３】　図１のサービス提供者側システムの構成を示すブロック図

【図４】　図１のサービスクライアント側システムの構成を示すブロック図

【図５】　秘密保持性が高い通信媒体によるコンテンツ情報供給制御を示すフローチャート

【図６】　認証処理に関連する構成を示すブロック図

【図７】　一般のネットワークによるコンテンツ情報供給制御を示すフローチャート

【図８】　鍵配送処理を示すタイムアロー図

【図９】　鍵配送処理に関連する構成を示すブロック図

【図１０】　鍵配送処理の内容を示すフローチャート

【図１１】　コンテンツ配送処理を示すタイムアロー図

【図１２】　ローカル課金処理の内容を示すフローチャート

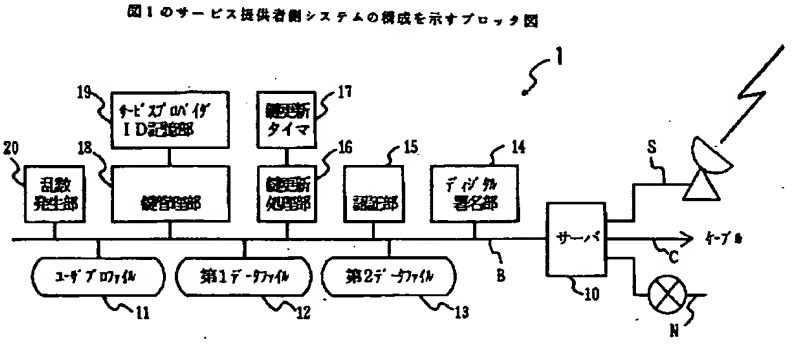
【図１３】　デジタル署名処理に関連する構成を示すブロック図

【図１４】　鍵の更新処理の内容を示すタイムアロー図

【符号の説明】

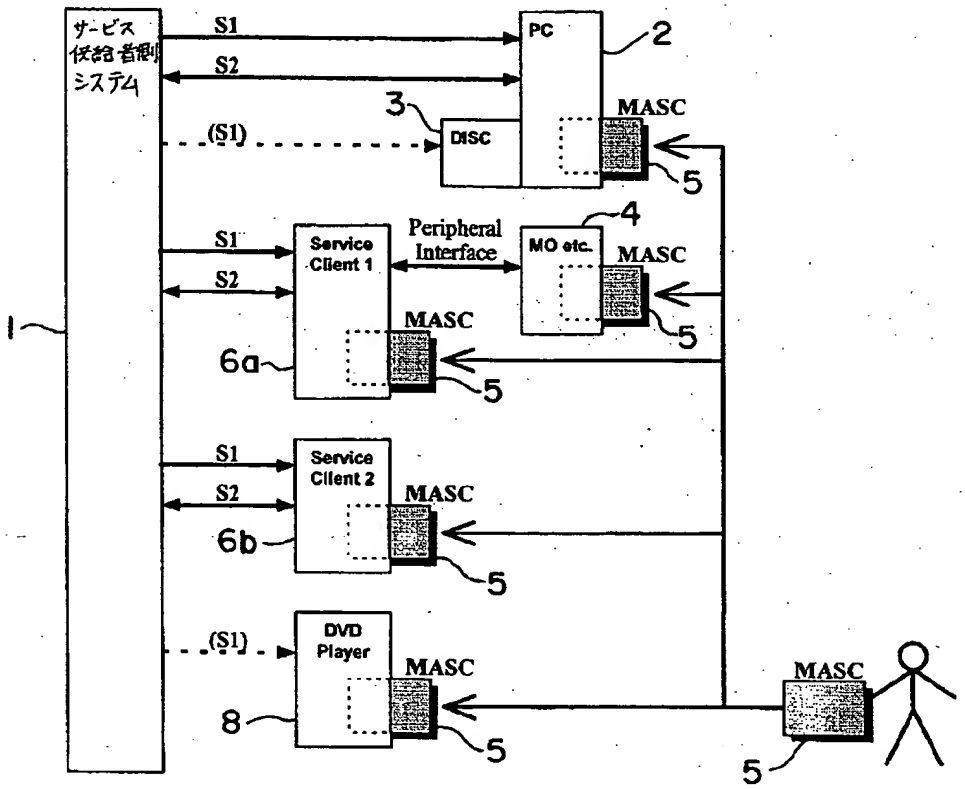
１	サービス提供者側システム
５	ＭＡＳＣ
６	サービスクライアント
１０	サーバ
１１	ユーザプロファイル
１２	第１データファイル
１３	第２データファイル
１４	デジタル署名部
１５	認証部
１６	鍵更新処理部
１８	鍵管理部
２０	乱数発生器
５３	ＤＥＳ
５５	課金情報記憶部
５７	ＲＯＭ

【図３】

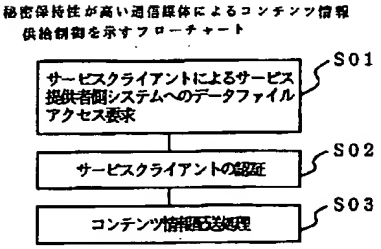


【図1】

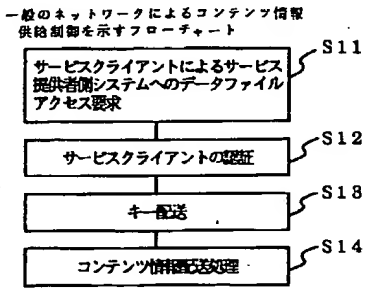
本発明の一実施例によるクライアント認証システムが適用されたデジタル・オーディオ・インタラクティブ・システムの概略図



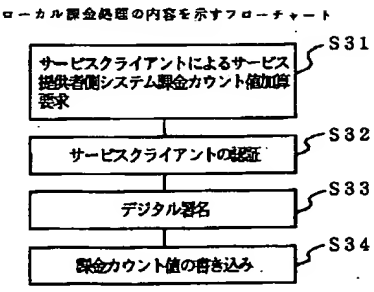
【図5】



【図7】

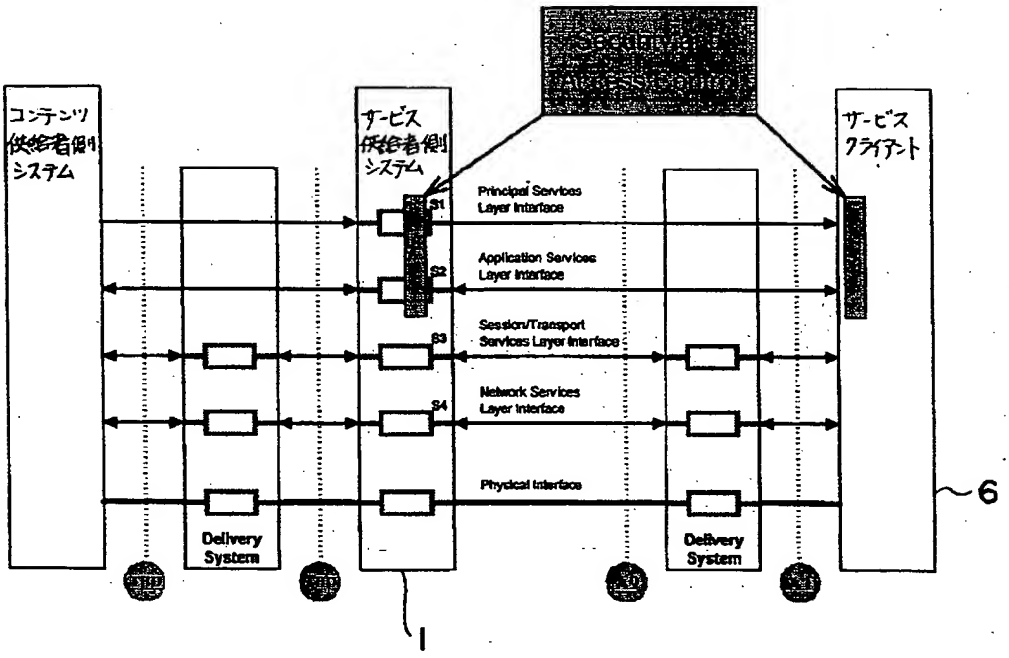


【図12】



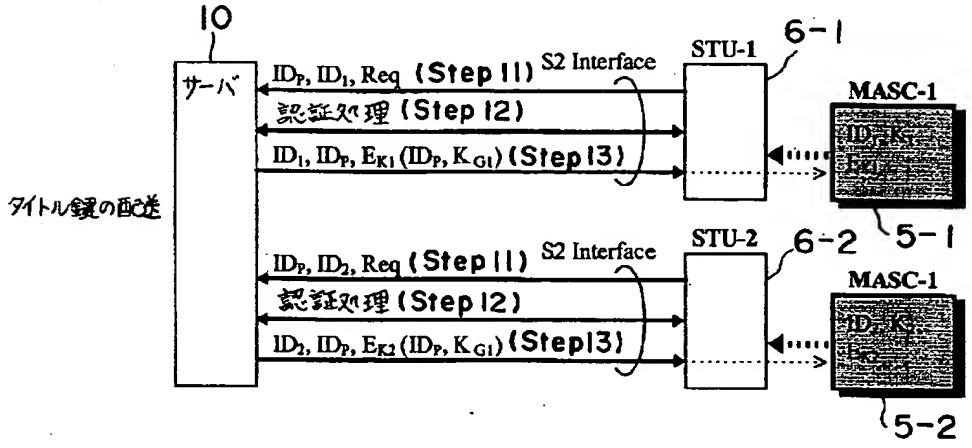
【図2】

図1のデジタル・オーディオ・インタラクティブ・システムに対応するシステムリファレンスモデルを示す図



【図8】

鍵配送処理を示すタイムアロー図



【図4】

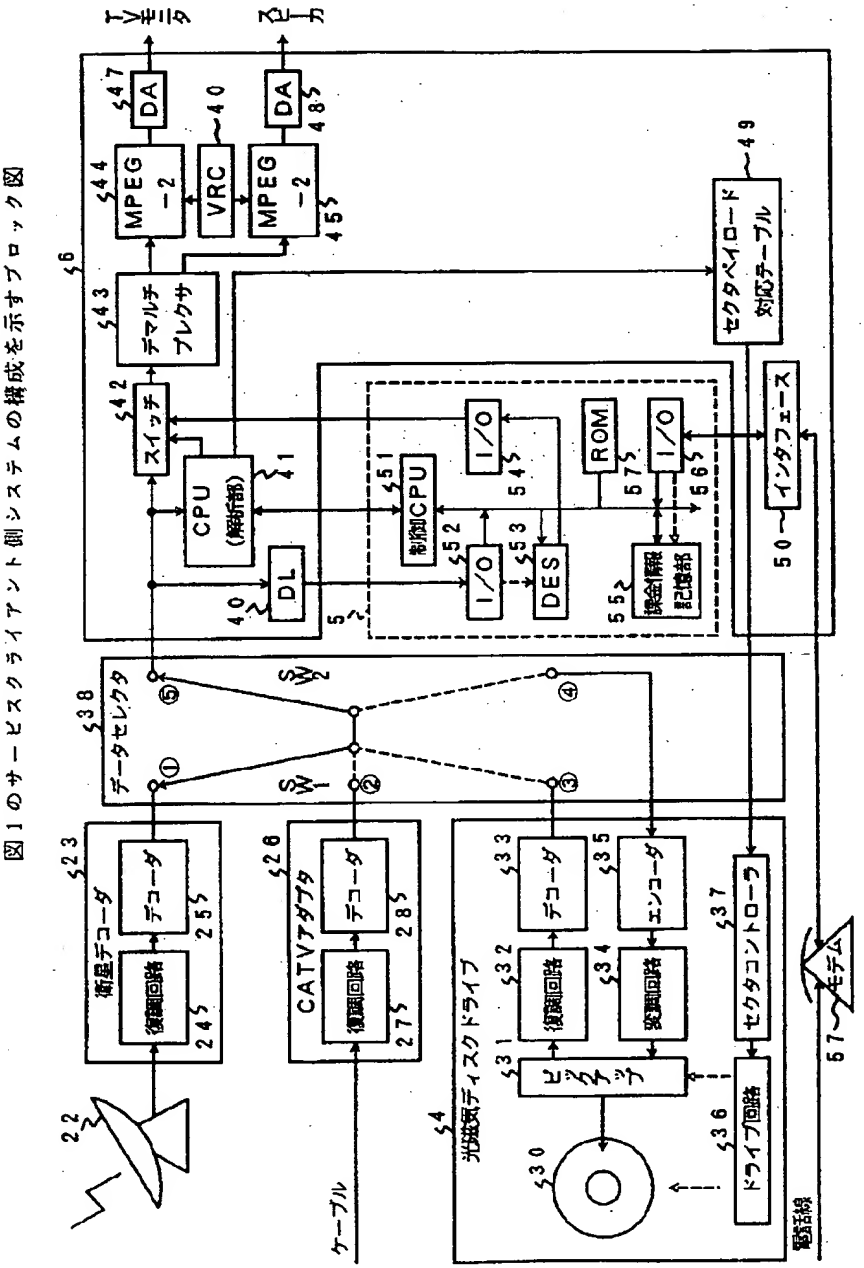
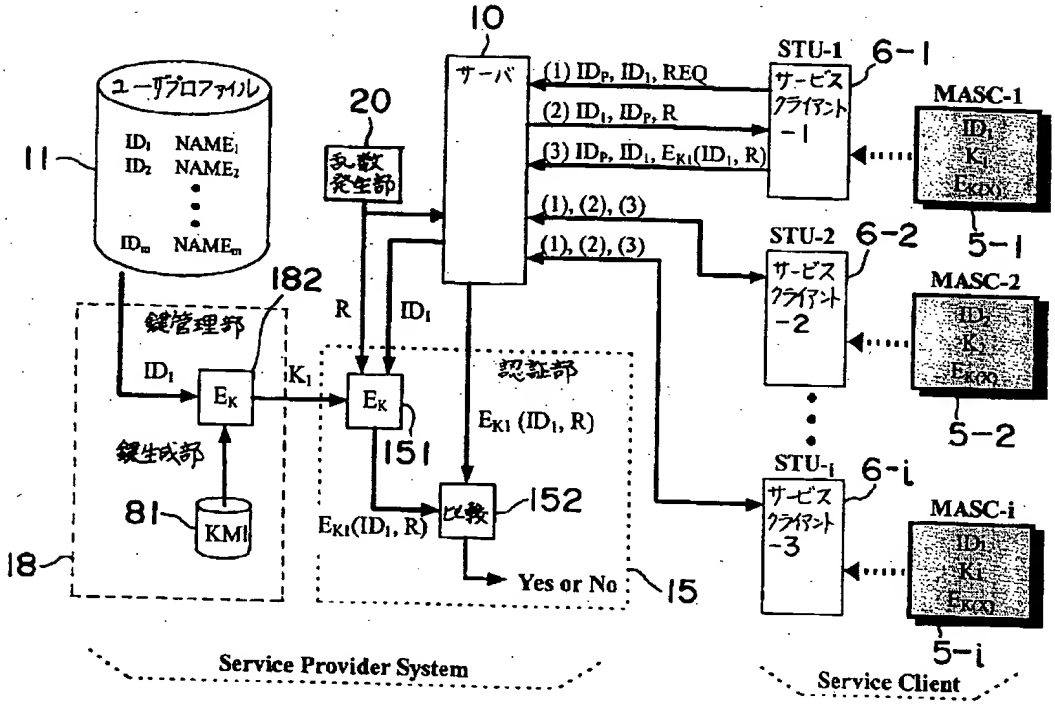


図1のサーバ・クライアント側システムの構成を示すブロック図
TVモニタ
スピーカ
DA
MPEG-2
VRC
MPEG-2
デマルチプレクサ
スイッチ
CPU（解析部）
DL
制御CPU
I/O
I/O
DES
ROM
I/O
課金情報記憶部
インタフェース
セクタペイロード対応テーブル
データセレクタ
衛星デコーダ
復調回路
デコーダ
CATVアダプタ
復調回路
デコーダ
光磁気ディスクドライブ
ピックアップ
復調回路
デコーダ
変調回路
エンコーダ
ドライブ回路
セクタコントローラ
モデム
電話線
ケーブル
SW1
SW2

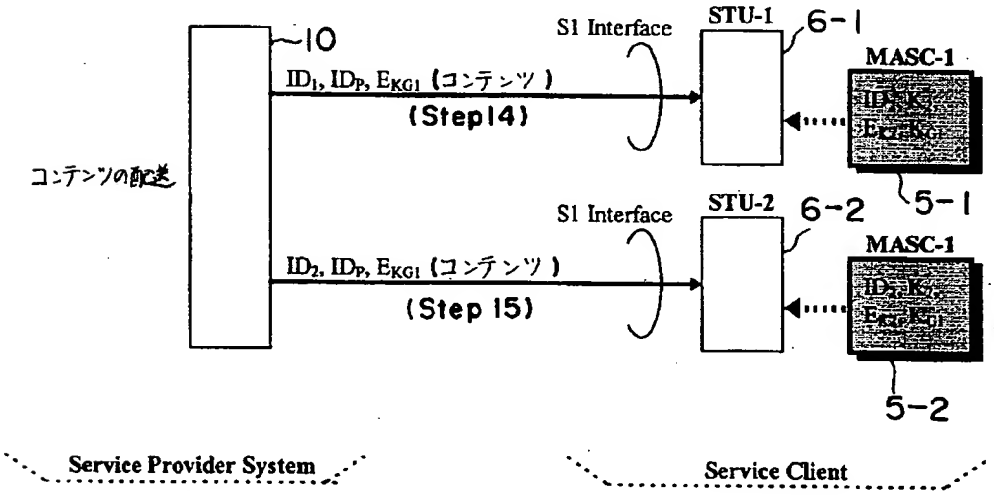
【図6】

認証処理に関連する構成を示すブロック図

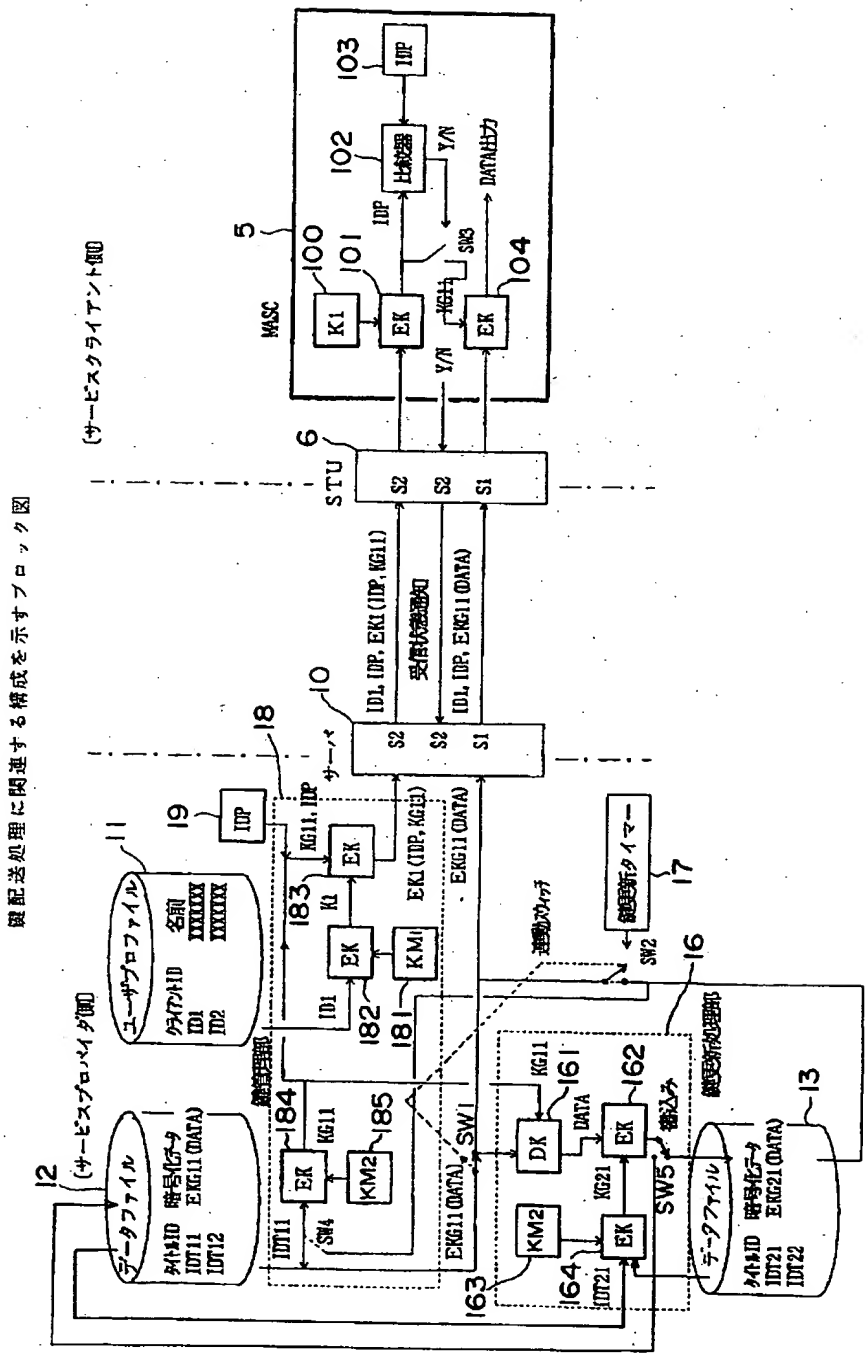


【図11】

コンテンツ配送処理を示すタイムアロー図



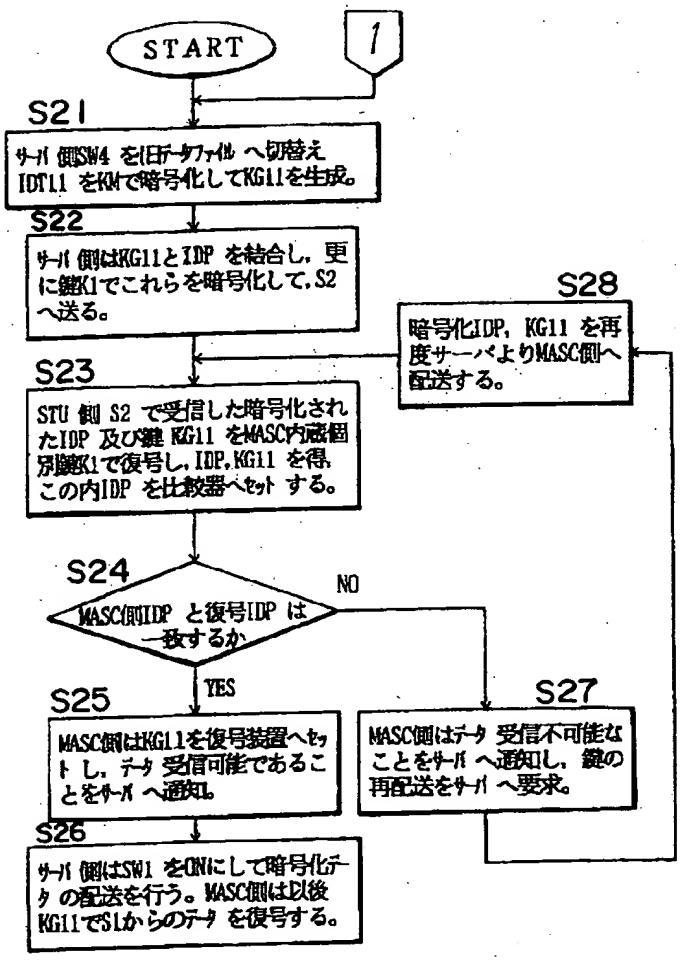
【図9】



鍵配送処理に関連する構成を示すブロック図

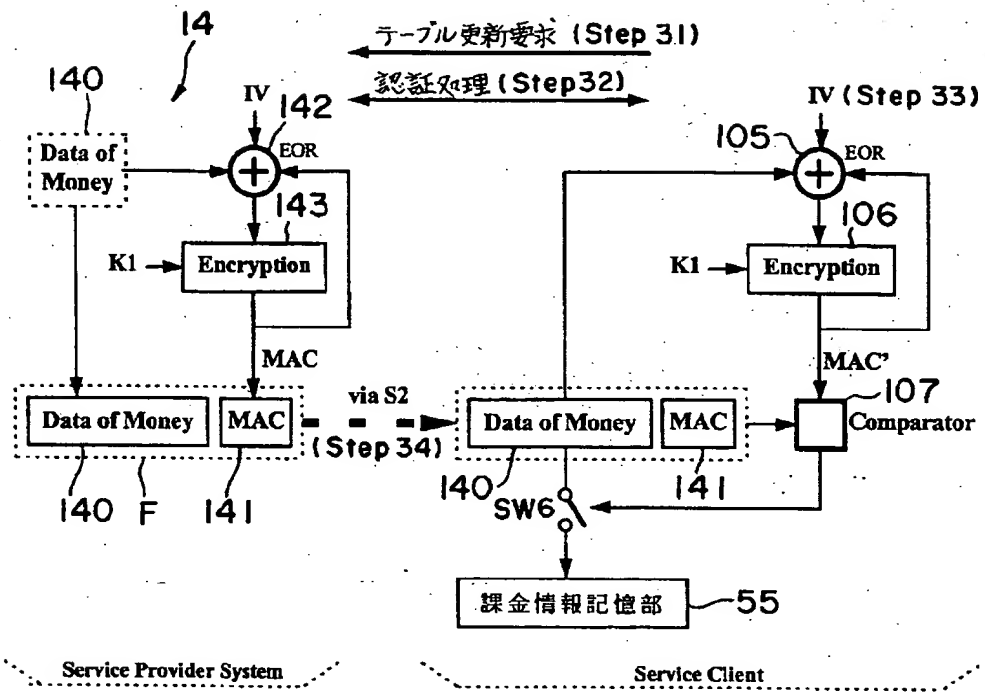
【図１０】

鍵配送処理の内容を示すフローチャート



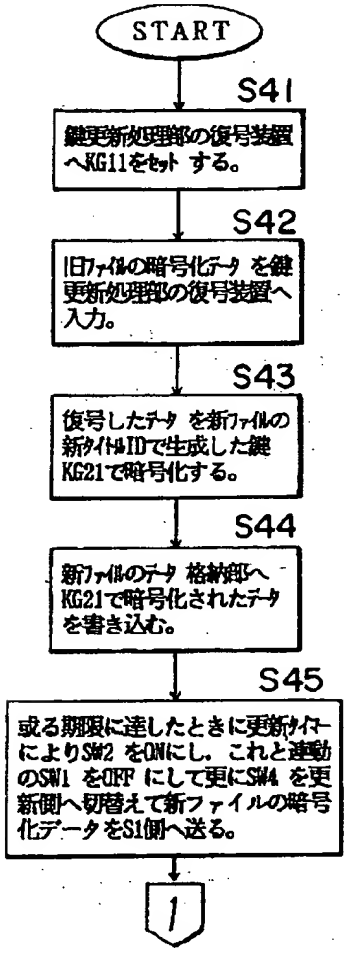
【図１３】

デジタル署名処理に関連する構成を示すブロック図



【図14】

鍵の更新処理の内容を示すタイムアロー図



フロントページの続き

(72)発明者　古賀　譲
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　石崎　正之
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内